What is claimed is:

1. A multicast delivery system comprising:

a delivery server which enciphers delivery data by using a current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data and a current use key identifier indicative of a pair of said current use cipher key and a current use decipher key as current use keys;

a key management server which is connected with said delivery server through a network, holds as a current use key data, a set of said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data in response to a current use key data request; and

a client terminal which is connected with said delivery server and said key management server through said network, receives said multicast packet from said deliver server, issues said current use key data request to said key management server to receive said current use decipherment key data from said key management server, holds said set of said current use decipher key and said current use key identifier, and deciphers said enciphered data contained in said multicast packet by using said current use decipher key when said current use key identifier contained in said multicast packet is coincident with said current use key identifier held in said client terminal.

2. The multicast delivery system according to claim 1, wherein said delivery server generates and holds as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, and transmits a set of said current use decipher key and said current use key identifier as said current use decipherment key data to said key management server, and

said key management server holds said current use decipher key and said current use key identifier as said current use decipherment key data.

3. The multicast delivery system according to claim 2, wherein said delivery server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining effective time data as said current use decipherment key data to said key management server,

said key management server holds said current use decipherment key data, and said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses.

4. The multicast delivery system according to claim 3, wherein said delivery server generates as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data, when said current use key remaining effective time data becomes a first present value, and transmits a set of said next use decipher key, said next use key identifier, and said next use key remaining effective time data to said key management server as a next use decipherment key data, and

said key management server holds said next use decipher key data.

5. The multicast delivery system according to claim 4, wherein said client terminal issues a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data from said key management server.

6. The multicast delivery system according to claim 5, wherein said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

7. The multicast delivery system according to claim 1, wherein said delivery server issues a current use key data generating request to said key management server,

said key management server generates and holds as a current use key data, a set of said current use cipher key, said current use decipher key and said current use key identifier in response to said current use key data generating request, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key data to said delivery server, and

said delivery server holds said current use encipherment key data.

8. The multicast delivery system according to claim 7, wherein said key management server sets a current use key remaining effective time data to said current use key data, and transmits a set of said current use decipher key, said current use key identifier, and said current use key remaining

effective time data as said current use encipherment key data to said delivery server,

said delivery server holds said current use encipherment key data, and

said delivery server, said key management server and said client terminal decreases said current use key remaining effective time data as time elapses.

9. The multicast delivery system according to claim 8, wherein said delivery server issues a next use key data generating request to said key management server, when said current use key remaining effective time data becomes a first present value,

said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier indicative of a pair of said next use cipher key and a next use key remaining effective time data in response to said next use key data generating request, and transmits a set of said next use encipher key, said next use key identifier, and said next use key remaining effective time data to said delivery server as a next use encipherment key data, and

said delivery server holds said next use encipherment key data.

10. The multicast delivery system according to

claim 9, wherein said client terminal issues a next use key request to said key management server when said current use key remaining effective time data becomes a second present value smaller than said first preset value, and receives and holds said next use decipherment key data of said next use decipher key, said next use key identifier, and said next use key remaining effective time data from said key management server.

11. The multicast delivery system according to claim 10, wherein said delivery server enciphers said delivery data by using said next use cipher key as said current use cipher key after said current use key remaining effective time data becomes 0.

12. The multicast delivery system according to claim 1, further comprising:

a plurality of said delivery servers; and

a plurality of said client terminals,

wherein each of said plurality of delivery server issues a next use key data generating request to said key management server while using said current use cipher key,

said key management server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, and transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and

said delivery server holds said next use encipherment key data.

13. The multicast delivery system according to claim 12, wherein each of said plurality of client terminals issues a next use decipher key request to said key management server when said client terminal does not hold said current use key identifier contained in said multicast packet,

said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and

said client terminal holds said next use decipherment key data.

14. The multicast delivery system according to claim 12, wherein each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients,

each of said plurality of client terminals issues a next use decipher key request to said key management server in response to said key data change previous notice,

said key management server transmits a set of said next use decipher key and said next use key identifier to said client terminal as a next use decipherment key data, and

said client terminal holds said next use decipherment key data.

15. The multicast delivery system according to claim 1, further comprising:

a plurality of said delivery servers; and

a plurality of said client terminals,

wherein said key management server comprises:

a master server; and

a plurality of slave servers,

wherein each of said plurality of delivery servers issues a next use key data generating request to said master server while using said current use cipher key,

said master server generates and holds as a next use key data, a set of a next use cipher key, a next use decipher key and a current use key identifier indicative of a pair of said next use cipher key and said next use decipher key in response to said next use key data generating request, transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to said delivery server, and transmits a set of said next use decipher key and said next use key identifier as a next use decipherment key data to said plurality of slave servers,

each of said plurality of slave servers holes said next use decipherment key data, and

said delivery server holds said next use encipherment key data.

16. The multicast delivery system according to claim 15, wherein each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers when said client terminal does not hold said current use key identifier contained in said multicast packet,

said slave server transmits said next use decipherment key data to said client terminal, and

said client terminal holds said next use decipherment key data.

17. The multicast delivery system according to claim 15, wherein each of said plurality of delivery servers issues a key data change previous notice to said plurality of clients,

each of said plurality of client terminals issues a next use decipher key request to any of said plurality of slave servers in response to said key data change previous notice,

said slave server transmits said next use decipherment key data to said client terminal, and

said client terminal holds said next use decipherment key data.

18. The multicast delivery system according to claim 1, wherein said key management server detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount.

19. The multicast delivery system according to claim 1, wherein said client terminal issues said key data request to said key management server, and

said key management server detects the number of said key data requests and charges a fee to said client terminal based on said detected number of key data requests.

20. A delivery server in a multicast delivery system, comprising:

a key data management table which holds a current use cipher key and a current use key identifier for said current use cipher key; and an enciphering section which refers to said key data management table to acquires said current use cipher key, enciphers delivery data by using said current use cipher key to generate enciphered data and transmits a multicast packet containing said enciphered data and said current use key identifier indicative of a pair of said current use cipher key and a current use decipher key as current use keys.

21. The delivery server according to claim 20, further comprising:

a key managing section which generates as a current use encipherment key data, a set of said current use cipher key, said current use decipher key and said current use key identifier, stores said current use cipher key and said current use key identifier in said key data management table, and transmits a set of said current use decipher key and said current use key identifier as a current use decipherment key data to a key management server.

22. The delivery server according to claim 20, further comprising:

a key managing section which generates as a current use encipherment key data, a set of said current use cipher key, said current use decipher key, said current use key identifier and a current use key remaining effective time data, stores said current use cipher key, said current use key identifier and said current use key remaining effective time data in said key data management table, and transmits a set of said current use decipher key, said current use key identifier and said current use key remaining effective time data as a current use decipherment key data to a key management server.

23. The delivery server according to claim 20, further comprising:

a key managing section which issues a next use key data generating request, and receives and stores a next use cipher key and a next use key identifier in said key data management table.

24. The delivery server according to claim 20, wherein said key data management table stores a current use key remaining effective time data in addition to said current use cipher key and said current use key identifier, and

said delivery server further comprises:

a key managing section which decrease said current use key remaining effective time data as time elapses, issues a next use key data generating request, when said current use key remaining effective time data becomes a first preset value, and receives and stores a next use cipher key and a next use key identifier in said key data management table.

25. The delivery server according to claim 20, further comprising:

a key managing section which issues a use key data change previous notice to client terminals, while using said current use cipher key.

26. A key management server in a multicast delivery system, comprising:

a key data management table which holds a current use decipher key and a current use key identifier for said current use decipher key; and

a key managing section which reads out said current use decipher key and said current use key identifier in response to a key data request to transmit to a request issuing client.

27. The key management server according to claim 26, wherein said key managing section generates as a current use key data, a set of a current use cipher key, said current use decipher key and said current use key identifier in response to a key data generating request, stores said current use key data in said key data management table, and transmits a set of said current use cipher key and said current use

key identifier as a current use encipherment key data to a request generating deliver server.

28. The key management server according to claim 27, wherein said key managing section generates as a next use key data, a set of a next use cipher key, a next use decipher key and a next use key identifier in response to a next key data generating request, stores said next use key data in said key data management table, and transmits a set of said next use cipher key and said next use key identifier as a next use encipherment key data to a request generating deliver server.

29. The key management server according to claim 26, wherein said key managing section receives said current use decipher key and said current use key identifier from a deliver server, and stores in said key data management table, and receives a next use decipher key and a next use key identifier from said deliver server, and stores in said key data management table.

30. The key management server according to claim 26, wherein said key data management table holds a current use key remaining effective time data in addition to said current use decipher key and said

current use key identifier, and

said key managing section decreases said current use key remaining effective time data as time elapses, reads out said current use decipher key, said current use key identifier and said current use key remaining effective time data in response to a key data request to transmit to a request issuing client.

31. The key management server according to claim 30, wherein said key managing section generates as a current use key data, a set of a current use cipher key, said current use decipher key, said current use key identifier and said current use key remaining effective time data in response to a key data generating request, stores said current use key data in said key data management table, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key data to a request generating deliver server.

32. The key management server according to claim 30, wherein said key managing section generates as a next use key data, a set of a next use cipher key, a next use decipher key, a next use key identifier and a next use key remaining effective time data in response to a next use key data generating request, stores said next use key data in said key data management table,

and transmits a set of said next use cipher key and said next use key identifier as a current use encipherment key data to a request generating deliver server.

33. The key management server according to claim 32, wherein said key managing section reads out said next use decipher key, said next use key identifier and said next use key remaining effective time data in response to a next use key data request to transmit to a request issuing client.

34. The key management server according to claim 30, wherein said key managing section receives said current use decipher key, said current use key identifier and a current use key remaining effective time data from a deliver server, stores in said key data management table, receives a next use decipher key, a next use key identifier and a next use key remaining effective time data from said deliver server, and stores in said key data management table.

35. The key management server according to claim 34, wherein said key managing section transmits a set of said next use cipher key, said next use key identifier and said next use key remaining effective time data as a next use encipherment key data to a

request generating deliver server.

36. The key management server according to claim 26, further comprising a key managing section detects a data amount of said multicast packets and charges a fee to said client terminal based on said detected data amount.

37. The key management server according to claim 26, further comprising a key managing section detects the number of said key data requests and charges a fee to said client terminal based on said detected number of key data requests.

38. A client terminal in a multicast delivery system, comprising:

a key data management table which holds a current use decipher key and a current use key identifier for said current use decipher key; and

a key managing section which issues a current use key data request to acquire a current use key data of said current use decipher key and said current use key identifier, stores said current use key data in said key data management table, determines whether a transmission key identifier contained in a multicast packet with an enciphered data is present in said key data management table, deciphers said enciphered data by using said decipher key stored in said key data management, when it is determined that said transmission key identifier is present, issues a next use key data request to acquire a next use key data of a next use decipher key and a next use key identifier, when it is determined that said transmission key identifier is not present, and stores said next use key data in said key data management table.

39. The client terminal according to claim 38, wherein said key data management table holds a current use key remaining effective time data in addition to said current use decipher key and said current use key identifier, and

said key managing section decreases said current use key remaining effective time data as time elapses, issues said next use key data request when said current use key remaining effective time data becomes a predetermined value, acquires said next use key data of said next use decipher key and said next use key identifier, and stores said next use key data in said key data management table.

40. A software product executable by a computer and storing a program executing functions of:

referring to a key data management table to acquire a current use cipher key;

enciphering delivery data by using said current use cipher key to generate enciphered data; and

transmitting a multicast packet containing said enciphered data and said current use key identifier indicative of a pair of said current use cipher key and a current use decipher key as current use keys.

41. The software product according to claim 40, wherein said program further executes the functions of:

generating a current use encipherment key data of said current use cipher key, said current use decipher key and said current use key identifier;

storing said current use cipher key and said current use key identifier in said key data management table; and

transmitting a set of said current use decipher key and said current use key identifier as a current use decipherment key data to a key management server.

42. The software product according to claim 40, wherein said program further executes the functions of:

generating a current use encipherment key data of said current use cipher key, said current use decipher key, said current use key identifier and a current use key remaining effective time data;

storing said current use cipher key, said current use key identifier and said current use key remaining effective time data in said key data management table, and transmits a set of said current use decipher key, said current use key identifier and said current use key remaining effective time data as a current use decipherment key data to a key management server.

43. The software product according to claim 40, wherein said program further executes the function of:

issuing a next use key data generating request, and receives and stores a next use cipher key and a next use key identifier in said key data management table.

44. The software product according to claim 40, wherein said program further executes the functions of:

storing a current use key remaining effective time data in addition to said current use cipher key and said current use key identifier in said key data management table;

decreasing said current use key remaining effective time data as time elapses;

issuing a next use key data generating request, when said current use key remaining effective time data becomes a first preset value; and

receiving and storing a next use cipher key and a next use key identifier in said key data management table.

45. The software product according to claim 40, wherein said program further executes the functions of:

issuing a use key data change previous notice to client terminals, while using said current use cipher key.

46. A software product executable by a computer and storing a program executing functions of:

storing a current use decipher key and a current use key identifier for said current use decipher key in a key data management table; and

reading out said current use decipher key and said current use key identifier in response to a key data request to transmit to a request issuing client.

47. The software product according to claim 46, wherein said program further executes the functions of:

generating as a current use key data, a set of a current use cipher key, said current use decipher key and said current use key identifier in response to a key data generating request; and

storing said current use key data in said key data management table, and transmits a set of said current use cipher key and said current use key identifier as a current use encipherment key data to a request generating deliver server.

48. The software product according to claim 47, wherein said program further executes the functions of:

generating as a next use key data, a set of a next use cipher key, a next use decipher key and a next use key identifier in response to a next key data generating request;

storing said next use key data in said key data management table; and

transmitting a set of said next use cipher key and said next use key identifier as a next use encipherment key data to a request generating deliver server.

49. The software product according to claim 46, wherein said program further executes the functions of:

receiving said current use decipher key and said current use key identifier from a deliver server;

storing in said key data management table;

receiving a next use decipher key and a next use key identifier from said deliver server; and

storing in said key data management table.

50. The software product according to claim 46, wherein said program further executes the functions of:

storing a current use key remaining effective time data in addition to said current use decipher key and said current use key identifier in said key data management table; and

decreasing said current use key remaining effective time data as time elapses; and

reading out said current use decipher key, said current use key identifier and said current use key remaining effective time data in response to a key data request to transmit to a request issuing client.

51. The software product according to claim 50, wherein said program further executes the functions of:

generating as a current use key data, a set of a current use cipher key, said current use decipher key, said current use key identifier and said current use key remaining effective time data in response to a key data generating request;

storing said current use key data in said key data management table; and

transmitting a set of said current use cipher key and said current use key identifier as a current use encipherment key data to a request generating deliver server.

52. The software product according to claim 50, wherein said program further executes the functions of:

generating a next use key data of a next use cipher key, a next use decipher key, a next use key identifier and a next use key remaining effective time data in response to a next use key data generating request;

storing said next use key data in said key data management table; and

transmitting a set of said next use cipher key and said next use key identifier as a current use encipherment key data to a request generating deliver server.

53. The software product according to claim 52, wherein said program further executes the functions of:

reading out said next use decipher key, said next use key identifier and said next use key remaining effective time data in response to a next use key data request to transmit to a request issuing client.

54. The software product according to claim 50, wherein said program further executes the functions of:

receiving said current use decipher key, said current use key identifier and a current use key remaining effective time data from a deliver server;

storing in said key data management table;

receiving a next use decipher key, a next use key identifier and a next use key remaining effective time data from said deliver server; and

storing in said key data management table.

55. The software product according to claim 54, wherein said program further executes the functions of:

transmitting a set of said next use cipher key, said next use key identifier and said next use key remaining effective time data as a next use encipherment key data to a request generating deliver server.

56. The software product according to claim 46, wherein said program further executes the functions of:

detecting a data amount of said multicast packets and charging a fee to said client terminal based on said detected data amount.

57. The software product according to claim 46, wherein said program further executes the functions of:

detecting the number of said key data requests and charging a fee to said client terminal based on said detected number of key data requests.

58. A software product executable by a computer and storing a program executing the functions of:

storing a current use decipher key and a current use key identifier for said current use decipher key in a key data management table; and

issuing a current use key data request to acquire a current use key data of said current use decipher key and said current use key identifier, stores said current use key data in said key data management table;

determining whether a transmission key identifier contained in a multicast packet with an enciphered data is present in said key data management table;

deciphering said enciphered data by using said decipher key stored in said key data management, when it is determined that said transmission key identifier is present;

issuing a next use key data request to acquire a next use key data of a next use decipher key and a next use key identifier, when it is determined that said transmission key identifier is not present; and

storing said next use key data in said key data management table.

59. The software product according to claim 58, wherein said program further executes the functions of:

storing a current use key remaining effective time data in addition to said current use decipher key and said current use key identifier in said key data management table;

decreasing said current use key remaining effective time data as time elapses;

issuing said next use key data request when said current use key remaining effective time data becomes a predetermined value;

acquiring said next use key data of said next use decipher key and said next use key identifier; and storing said next use key data in said key data management table.